PCT/RU98/00181

REC'D 16 SEP 1998

WIPO PCT

09762204 25 KU

РОССИЙСКОЕ АГЕНТСТВО ПО ПАТЕНТАМ И ТОВАРНЫМ ЗНАКАМ
(РОСПАТЕНТ)

ФЕДЕРАЛЬНЫЙ ИНСТИТУТ ПРОМЫШЛЕННОЙ СОБСТВЕННОСТИ

рег.No 20/14-347(3)

11 августа 1998 года

С П Р А В К А

Федеральный институт промышленной собственности Российского Агентства по патентам и товарным знакам настоящим удостоверяет, что приложенные материалы являются точным воспроизведением первоначального описания, формулы и чертежей (если имеются) заявки на выдачу патента на изобретение N 98107784, поданной в апреле месяце 22 дня 1998 года.

Название изобретения: Способ блочного шифрования двоичной информации.

Заявитель (и): МОЛДОВЯН Александр Андреевич.

Действительные авторы: МОЛДОВЯН Александр Андреевич,
МОЛДОВЯН Николай Андреевич,
САВЛУКОВ Николай Викторович.

PRIORITY DOCUMENT

Уполномоченный заверить копию
заявки на изобретение

Г.Ф.Востриков
Заведующий отделом

Экз. N ≙ 1

МПК[6] H 04 L 9/00

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДВОИЧНОЙ ИНФОРМАЦИИ

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования сообщений (информации). В совокупности признаков заявляемого способа используются следующие термины:

-ключ шифрования представляет из себя комбинацию битов, используемую при шифровании информационных сигналов данных; ключ шифрования является сменным элементом шифра и используется для преобразования данного сообщения или данной совокупности сообщений; ключ шифрования должен быть известным только законному пользователю;

-шифр представляет собой совокупность элементарных шагов преобразования входных данных с использованием шифрключа; шифр может быть реализован в виде программы для ЭВМ или в виде отдельного электронного устройства;

-подключ представляет собой часть ключа шифрования, используемую на отдельных элементарных шагах шифрования;

-двоичный вектор - это некоторая последовательность нулевых и единичных битов, например 101101011; конкретная структура двоичного вектора может быть интерпретирована как двоичное число, если считать, что позиция каждого бита соответствует двоичному разряду, т.е. двоичному вектору может быть сопоставлено численное значение, которое определяется однозначно структурой двоичного вектора;

-шифрование есть процесс, реализующий некоторый способ преобразования данных с использованием шифрключа, переводящий данные в

криптограмму, представляющую собой псевдослучайную последовательность знаков, из которой получение информации без знания ключа шифрования практически невыполнимо;

-дешифрование есть процесс, обратный процедуре шифрования; дешифрование обеспечивает восстановление информации по криптограмме при знании ключа шифрования;

-криптостойкость является мерой надежности защиты информации и представляет собой трудоемкость, измеренную в количестве элементарных операций, которые необходимо выполнить для восстановления информации по криптограмме при знании алгоритма преобразования, но без знания ключа шифрования.

Известны способы блочного шифрования двоичной информации, см. например стандарт США DES [У.Диффи, М.Э. Хеллмэн. Защищенность и имитостойкость: Введение в криптографию// ТИИЭР. 1979. Т. 67. N. 3. С. 87-89], способ шифрования по патенту США N 5222139, от 22 июня 1993 г., шифр FEAL-1 и криптоалгоритм B-Crypt [С.Мафтик. Механизмы защиты в сетях ЭВМ.- М., Мир, 1993. С. 49-52]. В известных способах шифрование блоков данных выполняют путем формирования ключа шифрования в виде совокупности подключей, разбиения преобразуемого блока данных на подблоки и поочередного изменения последних с помощью операций подстановки, перестановки и арифметических операций, выполняемых над текущим подблоком и текущим подключом.

Однако, известные способы-аналоги не являются достаточно стойкими к известному дифференциальному криптоанализу [Berson T.A. Differential Cryptanalysis Mod 2^{32} with application to MD5// EUROCRYPT'92. Hungary, May 24–28, 1992. Proceedings. P. 67-68], т.к. для всех входных блоков данных для заданного шага преобразования используется один и тот же подключ в неизменном виде.

Наиболее близким по своей технической сущности к заявляемому способу шифрования двоичной информации является способ, описанный в Российском стандарте криптографической защиты данных [Стандарт

СССР ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования]. Способ-прототип включает в себя формирование ключа шифрования в виде последовательности из 8 подключей длиной 32 бита, разбиении входного 64-битового блока данных на два 32-битовых подблока B_1 и B_2 и поочередном преобразовании подблоков. Один шаг преобразования подблока, например подблока B_2, заключается в наложении на на него текущего подключа Q_i, являющегося фиксированным для данного шага, с помощью операции сложения по модулю 2^{32} $(+)$ в соответствии с формулой $B_2 := B_2 + Q_i$, где $1 \leq i \leq 8$, после чего над полученным новым значением подблока B_2 выполняют операцию подстановки, затем операцию циклического сдвига влево на одиннадцать бит, т.е. на одиннадцать двоичных разрядов в сторону старших разрядов, а затем на полученное значение B_2 накладывают подблок B_1 с помощью операции поразрядного суммирования по модулю два $(\oplus)$ в соответствии с формулой $B_2 := B_2 \oplus B_1$. Операция подстановки выполняется следующим образом. Подблок разбивается на 8 двоичных вектора длиной по 4 бит. Каждый двоичный вектор заменяется двоичным вектором из таблицы подстановок. Выбранные из таблицы подстановок 8 4-битовых вектора объединяются в 32-битовый двоичный вектор, который и является выходным состоянием подблока после выполнения операции подстановки. Всего выполняется 32 аналогичных шага изменения подблоков, причем для всех преобразуемых входных блоков данных на фиксированном шаге преобразования подблоков используется один и тот же подключ с неизменным значением.

Однако, способ-прототип имеет недостатки, а именно, при программной реализации он не обеспечивает скорость шифрования более 1 Мбит/с [Андреев Н.Н. О некоторых направлениях исследований в области защиты информации// Сборник материалом международной конференции "Безопасность информации". Москва, 14-18 апреля 1997. М. 1997. С. 96], что не позволяет использовать его для шифрования данных в средствах защиты реального масштаба времени. Этот недостаток связан с тем,

что для обеспечения стойкости к дифференциальному криптоанализу в способе прототипе используется большое число операций подстановки над 4-битовыми подблоками преобразуемого блока данных, для выполнения каждой из которых (при программной реализации) микропроцессор осуществляет много элементарных команд, что обусловлено несоответствием подстановок такого типа с форматом представления данных в ЭВМ.

В основу изобретения положена задача разработать способ блочного шифрования двоичной информации, в котором преобразование входных данных осуществлялось бы таким образом, чтобы обеспечивалось уменьшение числа элементарных операций преобразования, приходящихся на один бит входных данных, при одновременном обеспечении высокой стойкости к дифференциальному криптоанализу, благодаря чему повышается скорость шифрования при программной реализации.

Поставленная задача достигается тем, что в способе блочного шифрования двоичной информации, включающем формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом новым согласно изобретению является то, что перед выполнением двухместной операции над i-тым подблоком и подключом над подключом выполняют операцию подстановки, зависящую от j-того подблока, где $j \neq i$.

Благодаря такому решению структура подключей, используемых на заданном шаге шифрования, зависит от преобразуемых данных и тем самым на данном шаге преобразования для различных входных блоков используются различные модифицированные значения подключей, благодаря чему обеспечивается высокая стойкость к дифференциальному криптоанализу при одновременном уменьшении числа выполняемых операций преобразования, что и обеспечивает повышение скорости криптографического преобразования.

Новым является также то, что в качестве выполняемой над подключом

операции подстановки, зависящей от j-го подблока, используют операцию подстановки, зависящую от ключа шифрования.

Благодаря такому решению обеспечивается дополнительное повышение стойкости шифрования при сохранении высокой скорости шифрования.

Ниже сущность заявляемого изобретения более подробно разъясняется примерами его осуществления со ссылками на прилагаемые чертежи.

Изобретение поясняется обобщенной схемой криптографического преобразования блоков данных на основе заявляемого способа, которая представлена фиг. 1, где: S – блок операции подстановки, зависящей от значения одного из преобразуемых подблоков; A и B – преобразуемые n-битовые подблоки; K_{2R}, K_{2R-1} – элементы ключа шифрования (подключи); знак$\oplus$ обозначает операцию поразрядного суммирования по модулю два, знак $\boxplus$ – операцию суммирования по модулю 2^n. Операционный блок S выполняет операцию подстановки над подключами K_{2R}, K_{2R-1} в зависимости от управляющего сигнала на управляющей шине, показанной прерывистой жирной линией. Жирные сплошные линии обозначают шину передачи n-битовых сигналов, а жирные пунктирные линии – шину передачи n управляющих сигналов, в качестве которых используются биты преобразуемых подблоков.

Фиг. 1 показывает один (R-тый) раунд шифрования. В зависимости от конкретной реализации блока управляемых подстановок и требуемой скорости преобразований могут быть заданы от 8 до 20 и более раундов.

Под операцией подстановки мы понимаем операцию замены двоичного значения сигнала на входе операционного блока S на другое двоичное значение (устанавливаемое на выходе операционного блока S), которое выбирается в зависимости от значения на входе блока S в соответствии с некоторой таблицей замены. Могут быть реализованы два варианта подстановок:

(1) n-битовый входной двоичный вектор заменяется на n-битовый выходной двоичный вектор, причем различным входным двоичным векто-

рам соответствуют различные выходные двоичные вектора;

(2) n-битовый двоичный вектор заменяется на m-битовый двоичный вектор, где $m \geq n$, причем различным входным двоичным векторам могут соответствовать как различные, так и одинаковые выходные двоичные вектора.

Операции подстановок обоих типов можно задать зависящими от некоторого управляющего сигнала, т.е. заданный двоичный вектор на входе может заменяться на различные выходные двоичные вектора в зависимости от значения управляющего сигнала, в качестве которого в заявляемом способе используется значение одного из преобразуемых подблоков.

Поясним задание зависимости операции подстановки первого типа от подблока преобразуемых данных . Пусть операции подстановки выполняются над двоичными векторами длиной n бит, где n - целое число. Тогда для определения операции подстановки размера nxn (обозначение nxn означает что входным для операции подстановки является блок данных размером n бит и выходным блоком также является двоичный вектор длиной n бит) требуется использование таблицы содержащей две строки чисел:

$$\begin{pmatrix} 0 & 1 & 2 & \dots & N-1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{N-1} \end{pmatrix},$$

где $N = 2^n$. В данной таблице в нижней строке присутствуют все возможные значения n-битового блока ровно по одному разу, но в произвольном порядке. Очередность расположения чисел в нижней строке определяет конкретный вариант таблицы подстановки, а следовательно и конкретный вариант операции подстановки, выполняемой с использованием этой таблицы. Выполнение операции подстановки осуществляется следующим образом. Выбирается в верхней строке число, которое равно значению входного блока. Находящееся под этим числом значение в нижней строке берется в качестве выходного блока. Таким образом, таблицу подстановки можно разместить в оперативной памяти ЭВМ как последовательную запись n-битовых компьютерных слов, размещенных

в ячейках с адресами $w_0, w_1, w_2, ..., w_{N-1}$. В этом случае значение входного двоичного вектора K служит для вычисления адреса $w_0 + K$ слова, которое берется в качестве выходного двоичного вектора. Этот способ представления таблицы подстановки требует использования объема памяти равного $2^n n$ бит. Выберем количество таблиц подстановки равное 2^L (объем требуемой памяти составит при этом $2^L Nn$ бит) и разместим таблицы подстановок непрерывно друг за другом. В качестве адреса таблицы с номером v возьмем значение адреса w_0 ее первого n-битового слова. Пусть адрес таблицы с номером $v = 0$ есть s. В этом случае адрес таблицы подстановки с любым номером v равен $s + vN$. Если задан управляющий двоичный вектор определяющий номер текущей таблицы подстановки v и текущий входной двоичный вектор, то операция подстановки выполняется заменой текущего входного блока на n-битовое слово, расположенное по адресу $s + vN + K$, где K - значение входного двоичного вектора, над которым выполняется текущая операция подстановки. Используя это соотношение легко задать выбор таблицы подстановки с номером v и выполнить подстановку над входным двоичным вектором со значением K. В рассмотренном случае задание зависимости таблиц подстановок от значения управляющего двоичного вектора и выполнение операции подстановки осуществляется микропроцессором очень быстро при выборе соответствующих значений параметров L и n, например при $L = 5$ и $n = 8$. При указанных параметрах для размещения таблиц подстановки требуется 8 Кбайт оперативной памяти, что является приемлемым, поскольку современные ЭВМ обладают объемом оперативной памяти на многие порядки больше этой величины (от 1 до 64 Мбайт и более).

Поясним задание зависимости операции подстановки второго типа от подблока преобразуемых данных на примере подстановок 8x32, задаваемых с помощью пронумерованной последовательности 32-битовых двоичных векторов $\{Q_j\}$, $j = 0, 1, 2, ..., 256$. Последовательность $\{Q_j\}$ может предполагаться известной и относящейся к описанию алгоритма шифро-

вания. В этом случае она может быть выработана по случайному закону, после чего она записывается как часть описания алгоритма шифрования. Другим вариантом задания последовательности $\{Q_j\}$ является ее генерирование по псевдослучайному закону в зависимости от ключа шифрования. В этом случае она является секретной, что дополнительно повышает криптостойкость шифрования. Преобразование 8-битового входного двоичного вектора (например, подключа) K осуществляется в зависимости от управляющего двоичного вектора (например, преобразуемого подблока) B следующим образом:
(1) вычисляется номер $j_0 = (B + K) \bmod 256$; (2) 8-битовый двоичный вектор K заменяется на 32-битовый двоичный вектор Q_{j_0}.

Рассмотрим конкретные примеры реализации заявляемого способа блочного шифрования двоичной информации.

Пример 1.

В данном примере поясняется шифрование 64-битовых блоков данных. Ключ шифрования формируется в виде 16 подключей K_1, K_2, K_3, ... K_{32}, каждый из которых имеет длину 32 бит. Входной блок данных разбивается на два 32-битовых подблока $A = a_4|a_3|a_2|a_1$ и $B = b_4|b_3|b_2|b_1$, представленные в виде конкатенации 8-битовых подблоков a_i и b_i, где $i = 1, 2, 3, 4$. Шифрование входного блока описывается следующим алгоритмом:

1. Установить счетчик числа раундов $r = 1$.
2. Преобразовать подблок B в соответствии с выражением:

$$B := B \oplus S_{a_1}(K_{8r}),$$

где $S_{a_1}(K_{8r})$ обозначает операцию подстановки над подключом K_{8r}, зависящую от подблока a_1.

3. Преобразовать подблок A в соответствии с выражением:

$$A := A + B \pmod{2^{32}}.$$

4. Преобразовать подблок A в соответствии с выражением:

$$A := A \oplus S_{b_1}(K_{8r-7}),$$

где $S_{b_1}(K_{8r-7})$ обозначает операцию подстановки над подключом K_{8r-7}, выполняемую в зависимости от подблока b_1.

5. Преобразовать подблок B в соответствии с выражением:

$$B := B + A \pmod{2^{32}}.$$

6. Преобразовать подблок B в соответствии с выражением:

$$B := B \oplus S_{a_2}(K_{8r-6}).$$

6. Преобразовать подблок A в соответствии с выражением:

$$A := A + B \pmod{2^{32}}.$$

7. Преобразовать подблок A в соответствии с выражением:

$$A := A \oplus S_{b_2}(K_{8r-5}).$$

8. Преобразовать подблок B в соответствии с выражением:

$$B := B + A \pmod{2^{32}}.$$

9. Преобразовать подблок B в соответствии с выражением:

$$B := B \oplus S_{a_3}(K_{8r-4}).$$

10. Преобразовать подблок A в соответствии с выражением:

$$A := A + B \pmod{2^{32}}.$$

11. Преобразовать подблок A в соответствии с выражением:

$$A := A \oplus S_{b_3}(K_{8r-3}).$$

12. Преобразовать подблок B в соответствии с выражением:

$$B := B + A \pmod{2^{32}}.$$

13. Преобразовать подблок B в соответствии с выражением:

$$B := B \oplus S_{a_4}(K_{8r-2}).$$

14. Преобразовать подблок A в соответствии с выражением:

$$A := A + B \pmod{2^{32}}.$$

15. Преобразовать подблок A в соответствии с выражением:

$$A := A \oplus S_{b_4}(K_{8r-1}).$$

16. Преобразовать подблок B в соответствии с выражением:

$$B := B + A \pmod{2^{32}}.$$

17. Если $r \neq 4$, то прирастить счетчик $r := r + 1$ и перейти к шагу 2, в противном случае СТОП.

В качестве таблицы подстановки, используемой для выполнения операции подстановки в примере 1 используется массив пронумерованных 32-битовых двоичных векторов $\{Q_j\}$, $j = 0, 1, 2, ..., 2048$. Для выполнения подстановки, например, над подключом K в зависимости от подблока a_i вычисляется значение номера j_a в соответствии с формулой $j_a = (K + a_i) \bmod 2^{11}$ и заменяется значение K на значение Q_{j_a}. Аналитически это записывается как $K := S_{a_i}(K)$.

Пример 2.

Этот пример полностью повторяет пример 1 за исключением того, что таблица $\{Q_j\}$, $j = 0, 1, 2, ..., 2048$, формируется до выполнения процедур шифрования в зависимости от ключа шифрования по псевдослучайному закону. Это можно сделать, например, следующим образом. Взять 1024 64-битовых двоичных вектора, имеющих численные значения 1,2, ..., 1024. Используя ключ шифования K_1, K_2,...,K_32, с помощью алгоритма шифрования RC5 [B.Schneier. Applied Cryptography/John Wiley & Sons, Inc., New York, 1996. P.344-345.] зашифруем указанные 64-битовые двоичные вектора. В результате получим набор 64-битовых блоков данных, имеющих псевдослучайные значения. Разбив каждый 64-битовый блок на два 32-битовых подблока получим псевдослучайную последовательность $\{Q_j\}$, $j = 0, 1, 2, ..., 2048$.

В современных ЭВМ операция извлечения двоичных векторов из оперативной памяти осуществляется за малое число машинных тактов, благодаря чему заявляемый способ обеспечивает скорость шифрования от 10 до 30 Мбит/с (в зависимости от конкретной реализации) для массового микропроцессора Pentium/200.

Приведенные примеры показывают, что предлагаемый способ блочного шифрования дискретной информации технически реализуем и позволяет решить поставленную задачу.

Заявляемый способ может быть реализован, например, в виде программ для ЭВМ, обеспечивающих скоростное шифрование данных.

Авторы:

Молдовян А.А

Молдовян Н.А.

Савлуков Н.В.

ФОРМУЛА ИЗОБРЕТЕНИЯ

1. Способ блочного шифрования двоичной информации, включающий формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом, о т л и ч а ю щ и й с я тем, что перед выполнением двухместной операции над i-тым подблоком и подключом над подключом выполняют операцию подстановки, зависящую от j-того подблока, где $j \neq i$.

2. Способ по п.1, о т л и ч а ю щ и й с я тем, что в качестве выполняемой над подключом операции подстановки, зависящей от j-го подблока, используют операцию подстановки, зависящую от ключа шифрования.

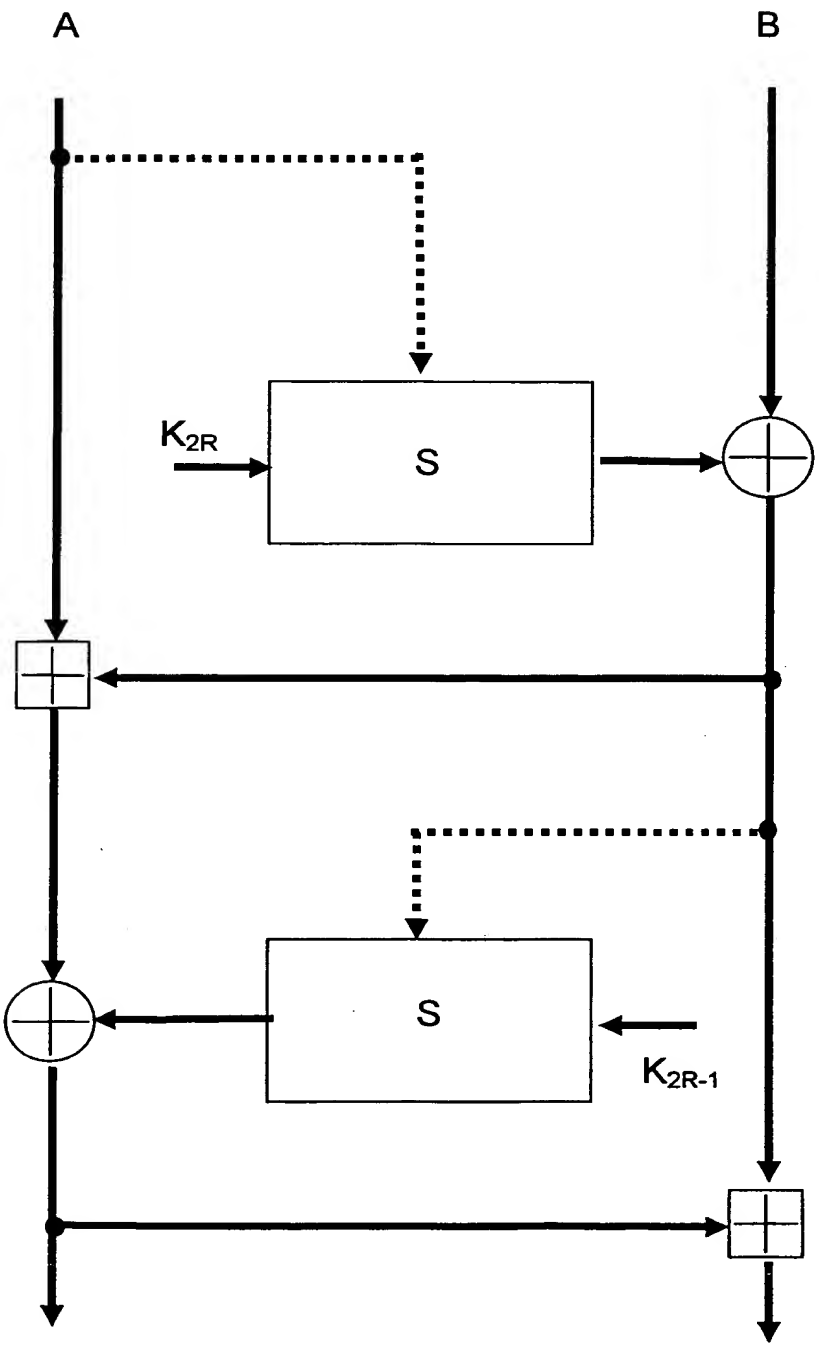
Авторы:

Молдовян А.А

Молдовян Н.А.

Савлуков Н.В.

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДВОИЧНОЙ ИНФОРМАЦИИ



Фиг.1.

Экз.N № 1

РЕФЕРАТ

СПОСОБ БЛОЧНОГО ШИФРОВАНИЯ ДВОИЧНОЙ ИНФОРМАЦИИ

Изобретение относится к области электросвязи и вычислительной техники, а конкретнее к области криптографических способов и устройств для шифрования данных. Целью изобретения является повышения скорости шифрования при программной реализации. Способ включает формирование ключа шифрования в виде совокупности подключей, разбиение блока данных на $N \geq 2$ подблоков и поочередное преобразование подблоков путем выполнения двухместной операции над подблоком и подключом. Новым в заявляемом способе является то, что перед выполнением двухместной операции над i-тым подблоком и подключом над подключом выполняют операцию подстановки, зависящую от j-того подблока, где $j \neq i$. Новым является также то, что в качестве выполняемой над подключом операции подстановки, зависящей от j-го подблока, используют операцию подстановки, зависящую от ключа шифрования.

Ф.и.-1, з.п.ф.и.-1, илл.-1